**Management Science and Engineering** 管理科学与工程, 2026, 15(4), 762-767
Published Online July 2026 in Hans. https://www.hanspub.org/journal/mse
https://doi.org/10.12677/mse.2026.154074

Hans汉斯

# AI工具赋能办公效能提升与保密风险防控策略

**赵克勇**

北京市农林科学院生物技术研究所，北京

收稿日期：2026年6月7日；录用日期：2026年6月29日；发布日期：2026年7月8日

## 摘　要

**人工智能(AI)技术通过智能决策优化管理工程流程，为现代办公模式革新注入新动能。科学选用适配的AI工具，能够显著优化办公流程、压缩事务处理时长，已成为提升办公效能的关键抓手；熟练掌握并应用AI工具，也逐步成为新时代办公岗位的核心职业素养。然而，AI工具开放共享的应用特性，也使得办公场景中涉及保密的信息面临泄露风险。因此，有必要构建完善的风险防控体系，以实现办公效能提升与保密安全的协同发展。**

## 关键词

**AI工具，办公效能，保密工作，风险防控，管理工程**

# Office Efficiency Improvement and Confidentiality Risk Prevention and Control Strategies under AI Tool Empowerment

**Keyong Zhao**

Institute of Biotechnology, Beijing Academy of Agriculture and Forestry Sciences, Beijing

Received: June 7, 2026; accepted: June 29, 2026; published: July 8, 2026

## Abstract

**Artificial intelligence (AI) technology optimizes the management of engineering processes through intelligent decision-making, injecting new momentum into the innovation of modern office models. The scientific selection of suitable AI tools can significantly optimize the office process and compress the transaction processing time, which has become the key to improve the office efficiency. Mastering**

文章引用: 赵克勇. AI 工具赋能办公效能提升与保密风险防控策略[J]. 管理科学与工程, 2026, 15(4): 762-767.
DOI: 10.12677/mse.2026.154074

**and applying AI tools skillfully has gradually become the core professional quality of office posts in the new era. However, the open and shared application characteristics of AI tools also pose a risk of information leakage in office scenarios involving confidentiality. Therefore, it is necessary to build a sound risk prevention and control system to achieve the coordinated development of office efficiency improvement and confidentiality security.**

## Keywords

**Artificial Intelligence Tools, Office Efficiency, Confidentiality Work, Risk Prevention and Control, Administrative Engineering**



## 1. 引言

在数字化转型的时代背景下，传统办公模式正面临效能提升的现实瓶颈。日常办公场景中经常充斥着大量重复性事务：报告撰写、合同编制、会议纪要整理等文档处理工作流程繁琐；数据筛选、分析与可视化呈现耗时费力；会议协调、邮件沟通及行政琐事进一步分散工作精力[1]。上述困境日益凸显，制约了单位整体办公工作效能的提升。

AI 技术的成熟应用为破解传统办公困境提供了全新路径。AI，即人工智能，它具有强大的学习和处理能力，能够模拟人类的思维和行为，完成许多复杂的任务[2]。依托强大的深度学习与信息处理能力，AI 可模拟人类逻辑思维完成复杂办公任务，覆盖文档智能生成、数据多维分析、邮件智能回复、业务流程自动化等多个办公场景，有效降低人力投入与时间消耗，实现办公效率的全方位提升[3] [4]。比如在文档撰写中，依托 ChatGPT、DeepSeek 等智能写作工具，仅需输入核心关键词或工作需求，即可快速生成结构完整、内容详实的文稿，省去逐字撰写与反复修改的繁琐流程；在数据处理领域，智能分析工具能够高效整合复杂数据，自动生成可视化图表与分析报告，挖掘数据背后的价值信息，在提升工作效率的同时减少人为疏漏，保障工作质量。

随着科技的不断发展，AI 技术在办公领域的应用已从基础文字处理延伸至复杂数据分析，从日常行政事务覆盖至核心决策支持，深度融入办公室工作全流程[5] [6]。借助 AI 技术推动办公模式革新，既是顺应时代发展的必然趋势，也是提升办公效能、增强竞争优势的必然选择。但数据安全与保密风险防范也不容忽视，当前数字化时代行业竞争日趋激烈，如何规范、安全、合理应用 AI 工具，已成为影响单位综合竞争力的重要因素。在此背景下，本文探讨 AI 工具在办公中的应用场景与潜在风险，提出兼顾办公效能提升与保密安全的优化策略，旨在为单位办公数字化与智能化转型提供参考。

## 2. AI 工具的办公应用场景

在数字化办公全面推进的背景下，AI 工具正以技术赋能的方式重塑办公室工作模式，推动办公流程的优化重组与整体效能的持续提升[7]。结合办公实际，AI 工具已在多类业务工作中展现出显著的应用价值，成为推动日常工作提质增效的重要支撑。

### 2.1. 智能写作类工具

公文起草、报告撰写、邮件往来等文字材料的编制，是办公室日常工作中频率高、耗时久的基础性事

务。智能写作工具的普及应用，有效化解了文字工作效率偏低的现实困境，为办公人员提供了便捷高效的内容创作支撑，目前，豆包、讯飞星火、文心一言、ChatGPT 等智能工具已在办公场景中得到广泛使用。

### 2.2. 数据处理类工具

数据整理与分析是办公场景的核心业务之一。面对大量复杂的数据信息，传统人工处理模式存在效率低下、误差率高、可视化呈现困难等短板，难以适配数字化时代的数据应用需求。以 ChatExcel 为代表的 AI 数据处理工具，实现了数据处理模式的革新，有效破解了传统数据处理中的各类问题。该类工具支持自然语言交互操作，工作人员无需掌握复杂的函数公式与专业操作技能，即可完成 Excel 数据的全流程处理。

### 2.3. 会议辅助类工具

会议是单位内部沟通、协同推进业务工作的重要载体，而会议记录、内容整理、任务跟进等环节往往耗时耗力，成为制约会议成效的突出因素。以讯飞听见、通义听悟为代表的 AI 会议辅助工具，依托智能语音识别与语义理解技术，为会议全流程管理提供了有效的解决方案。在会议进行过程中，该类工具能够实时将语音信息精准转译为文字，识别准确率高且转写速度快。同时，它们可对会议内容进行智能分析和结构梳理，自动提炼会议核心观点、关键决议及后续待办事项，并对重要节点信息进行智能标注，生成条理清晰的会议纪要。会议结束后，参会人员能够即时获取完整的会议文本资料，无需投入额外时间进行人工整理，有效压缩了事务性工作耗时。

### 2.4. 办公流程自动化工具

办公流程自动化工具依托 AI 与流程自动化技术，能够实现日程规划、邮件处理、合同审核等重复性办公事务的智能化处理，通过优化业务流转路径，减少人工干预环节，推动整体办公效能稳步提升。以日程智能规划为例，这类工具可根据员工的工作安排、会议日程、任务优先级等多项信息，自动生成科学合理的工作计划与日程方案，有效规避人工排期中易出现的时间冲突、任务失衡等问题。

## 3. 掌握并利用 AI 工具提升办公效能

### 3.1. 选择适合的 AI 工具

AI 工具种类繁多、功能各异，如何结合岗位需求筛选适配的智能工具，是办公智能化转型过程中需要重点关注的环节。工具选择的适配度直接决定技术赋能的效果，适配度越高，越能推动工作提质增效。例如在文字撰写、材料起草等工作中，豆包、ChatGPT 等智能写作类工具具备突出优势；在数据统计、信息分析、图表制作等工作中，ChatExcel、Tableau 等数据处理工具则能充分发挥效能[8]。

当然，在选择 AI 工具时，还应综合考量工具的操作门槛、功能完善度及系统兼容性。有的工具功能全面但操作逻辑复杂，学习成本较高，有的工具界面简洁、上手便捷，但核心功能存在一定局限。办公人员应立足岗位业务特点与实际应用场景，兼顾实用性与易用性进行筛选。同时，可结合行业评价、用户反馈等外部参考信息，全面了解工具的实际应用效果，提升选择的科学性与合理性。

### 3.2. 学习与应用 AI 工具

熟练掌握 AI 工具的操作逻辑与应用技巧，是释放其技术效能、赋能办公升级的核心前提。在日常学习过程中，办公人员可结合自身知识储备与岗位需求，依托官方文档、在线教程、视频课程等多元化学习资源，系统掌握各类 AI 工具的操作流程与核心功能。只有充分理解 AI 工具的功能特点，才能在日常工作中灵活运用，充分发挥其价值。

针对智能写作工具，应注重学习提示词设计技巧，通过精准、完整的需求描述，引导工具生成贴合

业务要求的内容。在使用 ChatGPT 等工具开展文稿创作时，可明确界定写作主题、行文结构、语言风格、字数要求等核心要素，借助清晰的指令获取高质量生成内容。在反复实践与交互训练中，持续优化沟通方式，逐步提升与智能工具的协同效率，最大化发挥技术赋能优势。

### 3.3. 与团队协作应用 AI 工具

团队协作是现代办公体系的核心环节，将 AI 工具深度融入团队协同工作体系，能够依托技术赋能优化业务流程，全面提升团队整体工作效能与跨岗位协作质量。团队内部可推行规范化的 AI 工具使用机制，明确业务处理流程与成果输出标准，推动成员熟练掌握工具操作逻辑，构建协同一致的工作模式。

团队成员可将工具使用技巧、高效提示词模板、业务场景解决方案等经验成果共享至资源库，形成团队专属的智能应用知识库。该库可作为交流研讨载体，促进成员分享应用心得、共研实操难题，通过知识互通、经验互鉴，实现团队整体 AI 应用素养的同步提升。

## 4. AI 工具办公应用面临的保密风险挑战

### 4.1. 数据安全风险

数据是人工智能技术运行的核心基础[9]。办公场景中大量业务信息、内部资料及涉密数据的接入，使得数据安全隐患随之凸显。AI 工具在模型训练与功能优化过程中会持续采集各类信息，部分平台存在数据采集范围超出业务必要范畴收集敏感信息与隐私内容。例如办公场景中语音转写、智能记录等功能在采集语音信号时，可能同步收录非业务相关的涉密对话与个人隐私内容，造成信息被动泄露。同样，数据存储与传输环节也存在明显的安全短板：承载智能办公数据的云端服务器易成为网络攻击的目标，办公文件和业务数据在交互传输过程中面临被非法截取、篡改、恶意利用的潜在威胁，这些情况进一步增加了涉密信息的安全风险。

### 4.2. 算法安全隐患

算法作为人工智能技术的运行内核，其自身的技术缺陷与逻辑偏差会直接转化为办公场景下的保密隐患[10]。部分智能算法在设计层面存在安全漏洞，不法分子可通过技术手段绕过安全防护体系，实施数据窃取、权限突破、恶意操控等违规行为。比如图像识别算法遭受针对性攻击后，可绕过门禁核验、身份识别等安全机制，突破企业物理及信息安全边界，威胁内部涉密区域与核心业务系统。此外，使用存在缺陷的数据训练出的模型，可能在信息处理过程中无意识泄露关键业务信息，或在智能决策、数据研判环节作出偏离客观事实的判断，不仅损害单位经营利益，也可能引发内部信息管控失衡，衍生出一系列保密安全问题。

### 4.3. 人员意识与管理问题

AI 办公模式的普及，对人员保密素养与单位管理体系提出了更高要求，认知不足与制度缺位成为当前保密风险的重要诱因。办公人员保密意识薄弱是风险产生的人为因素，部分人员未能充分认识 AI 工具应用过程中的数据安全隐患，缺乏信息保密的警惕性与专业性，日常工作中存在违规操作行为，如将包含工作机密、内部决策、涉密数据的文件被随意上传至外部未授权智能平台进行处理，为信息泄露埋下直接隐患。

## 5. 实现办公效能提升与保密安全兼顾的优化策略

### 5.1. 技术保障措施

#### 5.1.1. 采用数据加密技术实现安全管控

在数据采集、云端存储、跨平台传输等关键环节嵌入加密算法，采用对称加密与非对称加密相结合

的混合加密方式，对核心办公数据、涉密文件进行高强度加密处理。即便数据在传输过程中被非法窃取，也难以被破解利用，从源头阻断信息泄露风险。

#### 5.1.2. 检测算法与模型层面的潜在漏洞

建立常态化的算法安全检测机制，定期开展漏洞监测、风险评估与安全加固工作，第一时间修复算法设计缺陷。引入模型水印、数据溯源等技术手段，实现 AI 模型的版权保护与使用轨迹追踪，有效防范模型被非法复制、篡改与违规滥用。

#### 5.1.3. 搭建网络安全防护体系

部署防火墙、入侵检测系统、网络安全审查等专业防护设备，对外部网络攻击、恶意访问行为进行实时拦截与预警。通过优化网络访问权限、划分安全网络区域，实现办公系统与外部网络的安全隔离，全面保障 AI 系统运行环境与内部办公网络的稳定安全。

### 5.2. 管理与制度建设

#### 5.2.1. 构建严格的保密管理制度

清晰界定数据使用范围、分级分类标准与岗位权限，细化违规操作的处置流程与问责机制。通过权限分级管控敏感数据，严格限制涉密信息的访问、复制与传输权限，杜绝未经授权将内部数据、涉密文件上传至外部公共 AI 平台进行处理的违规行为。

#### 5.2.2. 强化供应商全流程管理

对 AI 技术服务商、平台供应商开展资质审核、安全能力评估与背景审查，签订标准化保密协议，明确双方数据安全责任与保密义务，要求供应商严格遵循内部保密规范。建立常态化安全审查机制，定期对供应商的数据处理流程、安全防护体系进行监督检查，及时规避外部合作中的信息泄露风险。

#### 5.2.3. 建立完善的应急响应体系

结合 AI 办公场景的风险特点，制定针对性的保密事件应急预案，明确数据泄露、系统入侵、信息篡改等突发事件的处置流程、责任分工与补救措施。通过定期开展应急演练，提升风险响应速度与处置能力，最大限度降低保密事故造成的损失。

#### 5.2.4. 编制安全 AI 工具应用清单

结合业务场景明确工具使用范围与使用规范，对涉及核心机密、敏感数据的业务环节划定工具使用红线，避免因工具滥用导致核心信息外泄。

### 5.3. 人员培训与教育

#### 5.3.1. 开展常态化保密意识专题培训

通过真实泄密案例剖析、行业风险通报、政策法规解读等形式，直观展现 AI 应用不当引发的信息安全隐患，引导员工树立常态化保密意识，摒弃侥幸心理，提升对涉密信息的辨别能力与风险警惕性。

#### 5.3.2. 开展针对性操作规范培训

围绕主流智能办公工具的安全使用方法、提示词设计规范、数据上传禁忌等内容开展实操培训，帮助员工熟练掌握安全、合规的操作技巧，规避因操作失误、认知偏差引发的保密风险，实现办公效率提升与信息安全管控的协同推进。

## 6. 结论与展望

AI 工具正在彻底改变传统办公体系，为提升办公效能开辟了新的可能。智能写作、数据处理、会议

辅助、流程自动化等工具，已深度融入办公的各个层面，成为业务优化和提升质量的关键支撑。这类工具不仅简化了繁琐的事务性工作，缩短了无效工作时长，还推动了办公模式向高效化、智能化转型。同时，AI 工具也促进了技术与团队协作的融合，加强了信息互通与跨岗位协同，为办公体系高质量发展奠定基础。

展望未来，随着算法优化、模型迭代与功能创新，AI 工具将更好地适配办公多元化需求，为办公工作提供高效、个性化的智能服务。办公人员应主动适应智能化转型趋势、保持常态化学习意识，掌握 AI 工具赋能价值。同时，要强化个人保密素养与规范操作能力，筑牢 AI 办公保密防线。只有紧跟技术发展步伐且坚守安全底线，才能充分释放 AI 技术的应用效能，提升行业核心竞争力。

## 参考文献

[1] 周亮, 冯甜甜. AI 驱动企业办公智能化转型[J]. 软件和集成电路, 2026(Z1): 56-58.

[2] 宋铁军. 未来 20 年都是 AI 时代[J]. 能源, 2017(5): 93-95.

[3] 雷海壮. 人工智能技术在企业办公服务中的应用研究[J]. 中国管理信息化, 2025, 28(18): 157-159.

[4] 周伟, 黄铁淳. 人工智能在政务服务创新中的应用[J]. 中国新通信, 2023, 25(18): 101-103+223.

[5] 路兴娜. “AI+财务”全方位赋能企业财务数智化升级[J]. 国际商务财会, 2026(8): 38-41+45.

[6] 姚迈新. AI 赋能行政领导决策能力优化探析——基于技术应用主体的视角[J]. 探求, 2025(4): 86-93.

[7] 张佩琳. 人工智能赋能高校办公室督办工作智能化转型[J]. 中国信息界, 2025(6): 114-116.

[8] 刘宇森. AI 在现代化办公场景中的应用现状研究与挑战[J]. 电脑采购, 2025(12): 61-63.

[9] 和军, 李江涛. 人工智能数据风险及其治理[J]. 中国特色社会主义研究, 2024(6): 42-51.

[10] 张爱军, 李圆. 人工智能时代的算法权力: 逻辑、风险及规制[J]. 河海大学学报(哲学社会科学版), 2019, 21(6): 18-24+109.